

MMS:GKS  
F.#2016R00088

UNITED STATES DISTRICT COURT  
EASTERN DISTRICT OF NEW YORK

**16M 757**

----- X  
IN THE MATTER OF THE SEARCH OF A  
BLACK LG CELLULAR PHONE, IMEI:  
014216-00-816447-3, SERIAL NO.  
510CQVU816447

AFFIDAVIT FOR A SEARCH  
WARRANT FOR AN  
ELECTRONIC DEVICE

----- X Case No. \_\_\_\_\_

**AFFIDAVIT IN SUPPORT OF AN  
APPLICATION UNDER RULE 41 FOR A  
WARRANT TO SEARCH AND SEIZE**

I, FINBARR FLEMING, being duly sworn, hereby depose and state as  
follows:

**INTRODUCTION AND AGENT BACKGROUND**

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—an electronic device—which is currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

2. I am a Task Force Officer with the Bureau of Alcohol, Tobacco, Firearms and Explosives (“ATF”) Joint Robbery Task Force, and have been since September 2014. I am responsible for conducting and assisting in investigations into the activities of individuals and criminal groups responsible for robberies. These investigations are conducted both in an undercover and overt capacity. I have participated in investigations involving search warrants and arrest warrants. In particular, I have participated in

investigations involving search warrants executed on cell phones. As a result of my training and experience, I am familiar with the techniques and methods used by individuals involved in criminal activity to conceal their activities from detection by law enforcement authorities.

3. I have personally participated in the investigation set forth below. I am familiar with the facts and circumstances of the investigation through my personal participation; from discussions with other agents and representatives of other law enforcement agencies; and from my review of records and reports relating to the investigation.

#### **IDENTIFICATION OF THE DEVICE TO BE EXAMINED**

4. The property to be searched is a BLACK LG CELLULAR PHONE, IMEI: 014216-00-816447-3, SERIAL NO. 510CQVU816447, hereinafter the "SUBJECT PHONE." The SUBJECT PHONE is currently located in the Eastern District of New York.

5. The applied-for warrant would authorize the forensic examination of the SUBJECT PHONE for the purpose of identifying electronically stored data particularly described in Attachment B.

#### **PROBABLE CAUSE**

6. On or about January 18, 2016, the defendants ADENE REID and CHARLES THOMAS were arrested by NYPD officers in connection with a commercial robbery that happened that day.

7. The defendants ADENE REID and CHARLES THOMAS were arraigned on January 19, 2016 before the Honorable Viktor V. Pohorelsky, United States Magistrate Judge for the Eastern District of New York. (16-MJ-48). REID and THOMAS were charged with violations of Title 18, United States Code, Sections 1951, 924(c) and 2.

8. On February 1, 2016, a grand jury in the Eastern District of New York returned a three-count indictment charging the defendants ADENE REID and CHARLES THOMAS with committing a Hobbs Act robbery and conspiring to commit the robbery, in violation of 18 U.S.C. § 1951 (Counts One and Two), and charging REID with brandishing a firearm in furtherance of these crimes of violence, in violation of 18 U.S.C. § 924(c) (Count Three).

9. During the robbery that occurred on January 18, 2016, two individuals, one later identified as the defendant ADENE REID and an Unknown Male, walked into an AT&T store located at 1169 Liberty Avenue in Brooklyn, New York at approximately 7:38 p.m. I have reviewed video surveillance footage from the store that reflects the events that transpired during the robbery. The footage captured images of REID wearing a mask and the Unknown Male wearing a scarf and a hood over his head. Once inside the store, both REID and the Unknown Male instructed store employees to take them to the store vault in the rear of the store. At the store vault, REID held open a bag into which a store employee was instructed to deposit store merchandise, in particular cellphones. The store employee deposited, among other things, Apple iPhones, Samsung Galaxy phones, tablets and United States currency.

10. Among the items collected by the defendant ADENE REID and the Unknown Male during the robbery was a security device implanted in a cellular telephone with Global Positioning System (“GPS”) capability. When this security device (the “Tracker Device”) is removed from the store, it automatically alerts enforcement and provide law enforcement with the ability to track its location in real-time in order to foil robberies.

11. After taking merchandise from the AT&T store, the defendant ADENE REID and the Unknown Male were captured on video surveillance footage walking out of the store.

12. Within a few minutes, the Tracker Device was activated and the NYPD received a notification that the Tracker Device was moving westbound along Atlantic Avenue in Brooklyn. NYPD officers responded and visually identified the make and model of the vehicle they determined was carrying the Tracker Device. The vehicle was a 2015 black Ford Edge, bearing the license plate number GZM7749 (the "Vehicle").

13. NYPD officers continued to visually track and follow the Vehicle carrying the Tracker Device. NYPD officers finally stopped the Vehicle near the corner of Decatur Street and Marcus Garvey Boulevard in Brooklyn.

14. Video surveillance footage recovered from a nearby home at the time of the Vehicle's stop captured: (1) an individual later identified as the defendant CHARLES THOMAS; (2) a person later identified as the defendant ADENE REID; and (3) the Unknown Male, exiting the vehicle. REID was later apprehended nearby at 148 Decatur Street in Brooklyn, New York. Shortly after the car stop, NYPD officers approached the Vehicle and observed THOMAS standing next to the passenger side door. Upon seeing NYPD officers approach, THOMAS fled on foot. NYPD officers apprehended THOMAS shortly thereafter near 1555 Fulton Street in Brooklyn, New York. THOMAS had keys to the Vehicle in his possession.

15. The Vehicle was seized and impounded on January 18, 2016. On January 20, 2016, Judge Pohorelsky issued a search warrant authorizing a search of the Vehicle and the seizure of, among other things, cellular telephones and other evidence of the

defendants ADENE REID's and CHARLES THOMAS' involvement in the robbery of the AT&T store located at 1169 Liberty Avenue in Brooklyn, New York.

16. On January 27, 2016, law enforcement agents executed the search warrant for the Vehicle and found, among other things, electronics that were stolen from the AT&T store as well as the SUBJECT PHONE. Law enforcement agents have confirmed that the electronics recovered by law enforcement agents were stolen from the AT&T store by comparing the electronics' unique identifying numbers with a list provided by the AT&T store.

17. The SUBJECT PHONE was discovered in the front passenger side center console cup holder of the Vehicle. The SUBJECT PHONE was not among the electronics stolen from the AT&T store. During the search of the Vehicle, law enforcement agents collected forensic swabs of possible DNA evidence from various locations in the Vehicle and, among other things, from the SUBJECT PHONE. The DNA evidence was submitted to an ATF forensic testing facility for testing. On August 11, 2016, the ATF forensic testing facility reported that the DNA of CHARLES THOMAS was found on the SUBJECT PHONE. Based on my training and experience, a determination that the DNA of a criminal suspect has been found on a phone found in the getaway car from a robbery makes it highly likely that the phone belongs to the suspect and/or was in his possession during the course of the robbery or the getaway.

18. Based on my training and experience, I know that co-conspirators to criminal activity commonly use mobile devices such as cellular telephones to communicate with each other through voice calls, text messages, emails, other electronic communications and other means. Further, I know that co-conspirators to the robbery of a commercial

establishment commonly use such mobile devices to plan and coordinate the robbery and its aftermath. Accordingly, there is probable cause to believe that on the SUBJECT PHONE are the items further described in Attachment B, which constitute evidence, fruits or instrumentalities of violations of 18 U.S.C. §§ 1951 and 924(c).

19. The SUBJECT PHONE is currently in the Eastern District of New York in the possession of law enforcement agents. In my training and experience, I know that the SUBJECT PHONE has been stored in a manner in which its contents are, to the extent material to this investigation, in substantially the same state as they were when the SUBJECT PHONE first came into the possession of law enforcement agents.

#### **TECHNICAL TERMS**

20. Based on my training and experience, I use the following technical terms to convey the following meanings:

- a. Wireless telephone (or mobile or cellular telephone): A handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving and storing text messages and email; taking, sending, receiving and storing still

photographs and video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system (“GPS”) technology for determining the location of the device, and a wide variety of applications, also known as “apps,” which may store the user’s preferences and other data. Such apps may include Facebook, Twitter and other social media services.

b. IP Address: An Internet Protocol address (or simply “IP address”) is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer or other electronic device, such as the SUBJECT PHONE, that connects to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

21. Based on my training, experience, and research, and from consulting the manufacturer’s advertisements and product technical specifications, I know that the SUBJECT PHONE provides not only phone and text message services, but can also be used to send and receive emails; access the Internet; track GPS data; take, store and share

photographs and videos; and use a wide variety of apps, such as Facebook, Twitter and many others. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the SUBJECT PHONE.

22. Based on my knowledge, training, and experience, I know that the SUBJECT PHONE can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the SUBJECT PHONE. This information can sometimes be recovered with forensics tools.

23. *Forensic Evidence.* As further described in Attachment B, this application seeks permission to locate not only data that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how the SUBJECT PHONE was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence can be recovered from the SUBJECT PHONE because:

a. Data on an electronic device can provide evidence of a file that was once on the device but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the device that show what tasks and processes were recently active. Web browsers, email programs, and instant messaging/“chat” programs store configuration information on the device that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the device was in use.



Electronic devices can record information about the dates files were created and the sequence in which they were created.

b. Forensic evidence on an electronic device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, registry information, configuration files, user profiles, email, email address books, instant messaging or chat logs, photographs, the presence or absence of malware, and correspondence (and the data associated with the foregoing, such as file creation and last-accessed dates) may be evidence of who used or controlled the electronic device at a relevant time.

c. A person with appropriate familiarity with how an electronic device works can, after examining this forensic evidence in its proper context, draw conclusions about how devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on an electronic device that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, such evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on an electronic device is evidence may depend on other information stored on the device and the application of knowledge about how the device behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding user attribution evidence, sometimes it is necessary to establish that a particular thing is not present on an electronic device. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

f. I know that when an individual uses an electronic device to violate 18 U.S.C. §§ 1951 and 924(c), the individual's electronic device may generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The electronic device is an instrumentality of the crime because it is used as a means of committing the criminal offense. The electronic device is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that an electronic device used to commit a crime of this type may contain: data that is evidence of how the device was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

24. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

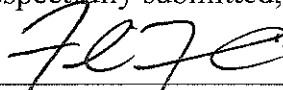
25. *Manner of execution.* Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does

not involve intrusion into a physical location. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

26. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the SUBJECT PHONE described in Attachment A to seek the items described in Attachment B.

Respectfully submitted,



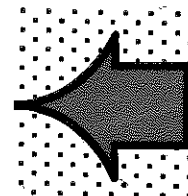
FINBARR FLEMING

Task Force Officer

ATF Joint Robbery Task Force

Subscribed and sworn to before me this  
16<sup>th</sup> day of August, 2016

THE H  
UNIT  
EAST  
S/TISCIONE  
TISCIONE  
JUDGE  
YORK



ATTACHMENT A

The property to be searched is a BLACK LG CELLULAR PHONE, IMEI: 014216-00-816447-3, SERIAL NO. 510CQVU816447 (the "SUBJECT PHONE"). The SUBJECT PHONE is currently located in the Eastern District of New York.

This warrant authorizes the forensic examination of the SUBJECT PHONE for the purpose of identifying the electronically stored information described in Attachment B.

**ATTACHMENT B**

All records on the SUBJECT PHONE described in Attachment A that relate to violations of Title 18, United States Code, Sections 1951 and 924(c) and involve ADENE REID and/or CHARLES THOMAS since December 15, 2015, including:

1. All records and information on the SUBJECT PHONE described in Attachment A, including names and telephone numbers, as well as the contents of all call logs, contact lists, text messages, emails (including those sent, received, deleted and drafted), instant messages, photographs, videos, Facebook posts, Internet activity (including browser history, web page logs, and search terms entered by the user), geo-location data, application data, and other electronic media;
2. Evidence of user attribution showing who used or owned the SUBJECT PHONE at the time the things described in this warrant were created, edited, or deleted, such as, for example, logs, phonebooks, saved usernames and passwords, documents, and browsing history;
3. Evidence of software that would allow others to control the SUBJECT PHONE, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
4. Evidence of the lack of such malicious software;
5. Evidence of the attachment to the SUBJECT PHONE of other storage devices or similar containers for electronic evidence;
6. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the SUBJECT PHONE;

7. Evidence of the times the SUBJECT PHONE was used;
8. Passwords, encryption keys, and other access devices that may be necessary to access the SUBJECT PHONE; and
9. Contextual information necessary to understand the evidence described in this attachment.

As used above, the terms “records” and “information” include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.